UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/649,678	08/28/2003	Natsume Matsuzaki	2003_1213A	5671

513 7590 06/04/2007

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
ALMEIDA, DEVIN E	

ART UNIT	PAPER NUMBER
2132	

MAIL DATE	DELIVERY MODE
06/04/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/649,678	MATSUZAKI ET AL.	
	Examiner	Art Unit	
	Devin Almeida	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *13 March 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-74* is/are pending in the application.

4a) Of the above claim(s) *1-2, 17, 35-48, 50-68* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *3-16,18-34,49 and 69-74* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This action is in response to the papers filed 3/13/2007. Claims 3-16, 18-34, 49, and 69-74 were received for consideration. Amendments for the claims were filed 3/13/2007. Currently claims 1, 2, 17, 35-48, and 50-68 have been cancelled claims 3-16, 18-34, 49, 69-74 are under consideration.

Response to Arguments

Applicant's arguments filed 2/21/2007 have been fully considered but they are not persuasive.

In response to applicant's argument that Yang does not disclose a valid period. The examiner disagrees Yang disclose in chapter 4 that the rekey interval T is a design parameter that a key is valid before it is replaced with a new key. Yang teaches that users are sent new keys that are valid for the interval T. A user who wishes to leave the group sends a request to leave the group to the group key management system and does not leave the group till the current key that the user has expires. The user leaving the group does not receive the new key and the number of users is reduced by one.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 3, 7, 10, 11, 13-15, 18, 19, 23, 28, 29, 49 and 69-74 are rejected under 35 U.S.C. 102(b) as being anticipated by Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis". With respect to claim 69, a group management device that manages a group, comprising: a reception unit operable to receive, from a member device, a request for registration in the group (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users as well as performs group rekeying); a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users), to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group (see chapter 2.4 Batch rekeying algorithms), (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group for the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval and chapter 4.3 System constraints and algorithm); and a communication unit operable, when judged in the affirmative, to output to the member device, the

common secret information and the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm).

With respect to claim 3, upon receiving the request, if the member device is authenticated as being the legitimate device, the judging unit judge whether the registered number of member devices is less than a maximum number of member devices registerable in the group, and when the judged in the affirmative, the judging unit registers the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 7, a generating unit operable to generate the common secret information, wherein the communication unit outputs the generated common secret information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 10, the maximum number is formed from a first maximum number and a second maximum number, and the judging unit judges whether the registered number is less than one of the first maximum number and the second maximum number, and registers the member device when judged in the affirmative (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 11, the first maximum number is the number of member devices, out of the maximum number, connectable to the group management device, and the second maximum number is the number of member devices, out of the maximum number, not connectable to the group management device, and the judging unit judges, (i) when the member device is connectable to the group management

device, whether the registered number of connectable member devices is less than the first maximum number, and (ii) when the member device is not connectable to the group management device, whether the registered number of non-connectable member devices is less than the second maximum number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 13, the judging unit functions to resist invalid access from outside, and the maximum number and the common secret information are stored in an area that is unreadable/unwritable from outside (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 14, the judging unit is included in a portable module that is mountable in the group management device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 15, the judging unit stores a remaining number obtained by subtracting the registered number from the maximum number, and on receipt by the reception unit of the registration request, judges whether the remaining number is "0", and when judged that the remaining number is not "0", the communication unit outputs the common secret information to the member device and the judging unit subtracts "1" from the remaining number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 17, the judging unit, when judged that the registered number is less than the maximum number, issues information showing a valid period during which use of the common secret information is permitted in the member device, increases the registered number, monitors the elapse of the valid period, and reduces

the registered number when the valid period ends, and the communication unit outputs the issued information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 18, the judging unit receives from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in accordance with the received number, and sets the received number as the maximum number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 19, the judging unit newly acquires from a management device outside of the group, a number of member devices registerable in the group, pays an accounting fee in accordance with the acquired number, and adds the acquired number to the maximum number to obtain a new maximum number (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 23, the communication unit stores therein the common secret information, newly receives a different piece of common secret information, overwrites the stored common secret information with the newly received common secret information, and outputs, regularly or irregularly, the newly received common secret information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 28, the received registration request requests the registration of a predetermined number of other member devices, the judging unit judges whether an aggregate number obtained by adding the predetermined number to the registered number is less than the maximum number, and when judged in the

affirmative, generates a permission right permitting a copying of the common secret information to the predetermined number of member devices, and the permission right is attached to the outputted common secret information (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 29, the received registration request includes a first identifier unique to the member device, the judging unit stores therein the first identifier, the reception unit, after the outputting of the common secret information, receives a second identifier unique to the member device, the judging unit judges whether the second identifier matches the first identifier, and the communication unit, when judged that the first and second identifiers match, again outputs the common secret information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3).

With respect to claim 49, a member device that user a content after registering in a group managed by a group managing device comprising: a requesting unit operable to request the group management device for registration in the group (see chapter 2 improving rekey encoding scalabilty i.e. a user can send a join request to the key server); a receiving unit operable to be authenticated by the group management device, and to receive, from the group management device, the common secret information and the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm); and a holding unit operable to hold the received common secret information, to monitor the elapse of the valid period, and to delete the common secret information when the valid period ends (see chapter 1

introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm).

With respect to claim 70, a group formation/management system comprising: a group management device (see chapter 1 introduction i.e. a group management system); and a group member device (see chapter 1 introduction i.e group key to authorized new users), the group management device including: a reception unit operable to receive, from a member device, a request for registration in the group (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users as well as performs group rekeying); a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users), to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group (see chapter 2.4 Batch rekeying algorithms), (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group for the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) to monitor an elapse of the valid

period and reduce the registered number when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval and chapter 4.3 System constraints and algorithm); and a communication unit operable, when judged in the affirmative, to output to the member device, the common secret information and the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm). the group member device including: a requesting unit operable to request the group management device for registration in the group (see chapter 2 improving rekey encoding scalabilty i.e. a user can send a join request to the key server); a receiving unit operable to be authenticated by the group management device, and to receive, from the group management device, the common secret information and the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm); and a holding unit operable to hold the received common secret information, to monitor the elapse of the valid period, and to delete the common secret information when the valid period ends (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm).

With respect to claim 71, a group management method used in a group management device that manages a group, the group management method comprising: receiving from a member device, a request for registration in the group (see chapter 2

improving rekey encoding scalabilty i.e. a user can send a join request to the key server); (i) upon receiving the request, if the member device is authenticated as being a legitimate device (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users), to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group (see chapter 2.4 Batch rekeying algorithms), (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group for the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) monitoring an elapse of the valid period and reducing the registered number when the valid period ends (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm); and when judged in the affirmative, outputting to the member device the common secret information and the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm).

With respect to claim 72, a recording medium storing a computer program used in a group management device that manages a group, the computer program

comprising: receiving from a member device, a request for registration in the group (see chapter 2 improving rekey encoding scalabilty i.e. a user can send a join request to the key server); (i) upon receiving the request, if the member device is authenticated as being a legitimate device (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users), to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group (see chapter 2.4 Batch rekeying algorithms), (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group fox the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) monitoring an elapse of the valid period and reducing the registered number when the valid period ends (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm); and when judged in the affirmative, outputting to the member device the common secret information and the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm).

With respect to claim 73, a control method used in a group management device that manages a group, the control method comprising: requesting the group management device for registration in the group (see chapter 2 improving rekey encoding scalabilty i.e. a user can send a join request to the key server); being authenticated by the group management device and receiving, from the group management device, common secret information unique to the group that includes valid period information showing a valid period of use of the common secret information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm); and holding the received common secret information, monitoring an elapse of the valid period, and deleting the common secret information when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm).

With respect to claim 74, a recording medium storing a computer program used in a group management device that manages a group, the computer program comprising: requesting the group management device for registration in the group (see chapter 2 improving rekey encoding scalabilty i.e. a user can send a join request to the key server); being authenticated by the group management device and receiving, from the group management device, common secret information unique to the group that includes valid period information showing a valid period of use of the common secret information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter

4.3 System constraints and algorithm); and holding the received common secret information, monitoring an elapse of the valid period and deleting the common secret information when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 3-6 and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et all: "Keystone: A Group Key Management Service" in view of Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis". With respect to claim 69, Wong teaches a group management device that manages a group, comprising: a reception unit operable to receive, from a member device, a request for registration in the group (see chapter 1 Introduction group key management and chapter 3.1 Registrar setup); a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device (see chapter 3.1 Registrar setup and 3.2 Client registration), to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group (see chapter 2), a communication unit operable, when judged in the affirmative, to output to the member device, the common secret information (see chapter 3 Keystone Architecture). Wong

does not teach (ii) when judged in the affirmative, to issue valid period information showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends; and to output to the member device, the valid period information. Yang teaches (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group for the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval and chapter 4.3 System constraints and algorithm); and to output to the member device, the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have the rekey interval as a system design parameter that a group key management system can use to control bandwidth overhead (see chapter 4.3 System constraints and algorithm). Therefore one would have been motivated to have the common secret have a valid period.

With respect to claim 3, upon receiving the request, if the member device is authenticated as being the legitimate device, the judging unit judge whether the registered number of member devices is less than a maximum number of member devices registerable in the group, and when the judged in the affirmative, the judging unit registers the member device (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

With respect to claim 4, the judging unit includes: an authentication subunit operable to hold a second initial value, and to authenticate the member device, using the second initial value and a first initial value held by the member device; and a device-number judging subunit operable, when authentication is successful, to judge whether the registered number is less than the maximum number, the common secret information outputted by the communication unit shows "registered in the group", and the member device receives and holds the outputted common secret information, and deactivates the first initial value (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

With respect to claim 5, the first and second initial values show "unregistered in the group" (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

With respect to claim 6, the first and second initial values show "unregistered in any group" (see Wong chapters 1, 3.1, 3.2, 3.3, and 4).

Claims 8 and 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis" in view of Steiner et al: "Cliques: A New approach to Group Key Agreement". Yang teaches everything with respect to claim 3 above but with respect to claim 8, the judging unit receives the

common secret information from the out-group management device, and the communication unit outputs the received common secret information to the member device (see Yang, abstract, chapter 1, 2.4, 4.2, and 4.3). Yang does not teach the common secret information is generated by a management device outside of the group. Steiner teaches the common secret information is generated by a management device outside of the group (see Steiner chapters 2, 3, and 5.2). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have a centralized key generation agreement since it is the most intuitive and most nature (see chapter 2). Therefore one would have been motivated to have the common secret information is generated by a management device outside of the group.

With respect to claim 9, the reception unit, on receipt of the registration request, notifies the receipt to a management device outside of the group, the out-group management device judges whether the registered number is less than the maximum number, the judging unit, instead of judging whether the registered number is less than the maximum number, receives a judgment result from the out-group management device, and the communication unit outputs the common secret information to the member device, when the judgment result shows that the registered number is less than the maximum number (see Steiner chapters 2, 3, and 5.2).

Claims 3, 12 and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Paolo (UK Patent application GB 2343025) in view of Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis". With respect to claim 69, Paolo teaches a

group management device that manages a group , comprising: a reception unit operable to receive, from a member device, a request for registration in the group (see figure 3 and page 5 lines 4-29 i.e. when a request is received from a client); a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group (see page 5 lines 4-29 i.e. the server creates a new license instance record and decrements by one the number of available licenses), a communication unit operable, when judged in the affirmative, to output to the member device, the common secret information (see page 5 lines 4-29 i.e. the server sends a reply to the client authorizing the client to use the software). Paolo does not teach (ii) when judged in the affirmative, to issue valid period information showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends; and to output to the member device, the valid period information. Yang teaches (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group for the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) to monitor an elapse of the valid period and reduce the registered

number when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval and chapter 4.3 System constraints and algorithm); and to output to the member device, the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have the rekey interval as a system design parameter that a group key management system can use to control bandwidth overhead (see chapter 4.3 System constraints and algorithm). Therefore one would have been motivated to have the common secret have a valid period.

With respect to claim 3, upon receiving the request, if the member device is authenticated as being the legitimate device, the judging unit judge whether the registered number of member devices is less than a maximum number of member devices registerable in the group, and when the judged in the affirmative, the judging unit registers the member device (see Paolo page 5 lines 4-29).

with respect to claim 12 does not teach the communication unit outputs to another group management device, a request inquiring whether the member device is registerable in the other group management device, the other group management device receives the inquiry request, judges whether a registered number of member devices is less than a maximum number of member devices registerable with the other group management device, and when judged in the affirmative, registers the member device and outputs the common secret information to the group management device,

and the communication unit, on receipt of the common secret information from the other group management device, outputs the received common secret information to the member device (see Paolo Figure 3 and page 1 line 6 – page 5 line 29).

Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis" in view of Canetti et al: "Multicast Security: A Taxonomy and Some Efficient Construction". Yang teaches everything with respect to claim 3 above but with respect to claim 16 does not teach the reception unit, after the outputting of the common secret information, receives from the member device, a request for withdrawal from the group, the communication unit, on receipt by the reception unit of the withdrawal request, outputs to the member device, a notification indicating to delete the common secret information, the reception unit receives from the member device, a notification showing that deletion of the common secret information has been completed, and the judging unit, on receipt by the reception unit of the deletion-completed notification, reduces the registered number. Canetti teaches the reception unit, after the outputting of the common secret information, receives from the member device, a request for withdrawal from the group, the communication unit, on receipt by the reception unit of the withdrawal request, outputs to the member device, a notification indicating to delete the common secret information, the reception unit receives from the member device, a notification showing that deletion of the common secret information has been completed, and the judging unit, on receipt by the reception unit of the deletion-completed notification, reduces the registered

number. (see Canetti see chapter 4 i.e. deletion of group key). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have the user leaving the group delete their group key to conceal future communication from the former member (see chapter 4). Therefore one would have been motivated to have the former member delete the common secret information.

Claims 3, 20-22, 24-27, 34 and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yevgeny (UK Patent application GB 2353682) in view of Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis". With respect to claim 69, Yevgeny teaches a group management device that manages a group , comprising: a reception unit operable to receive, from a member device, a request for registration in the group; a judging unit operable, (i) upon receiving the request, if the member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, a communication unit operable, when judged in the affirmative, to output to the member device, the common secret information (see page 7 line 25 – page 8 line 2 page 10 lines 11-16 page 19 line 23 – page 20 line 24). Yevgeny does not teach (ii) when judged in the affirmative, to issue valid period information showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends; and to output to the member

device, the valid period information. Yang teaches (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group for the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval and chapter 4.3 System constraints and algorithm); and to output to the member device, the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm). It would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains to have the rekey interval as a system design parameter that a group key management system can use to control bandwidth overhead (see chapter 4.3 System constraints and algorithm). Therefore one would have been motivated to have the common secret have a valid period.

With respect to claim 3, upon receiving the request, if the member device is authenticated as being the legitimate device, the judging unit judge whether the registered number of member devices is less than a maximum number of member devices registerable in the group, and when the judged in the affirmative, the judging

unit registers the member device (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 20, the reception unit, after the outputting of the common secret information, receives a communication request from the member device, the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and the communication unit communicates with the member device when authentication is successful (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 21, a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key; and an encryption unit operable to encrypt the content key using a key generated based on the common secret information, to generate an encrypted content key, wherein the communication unit outputs the encrypted content and the encrypted content key to the member device (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 22, the judging unit authenticates the member device using the common secret information and common secret information held by the member device, and shares a session key with the member device, using the common secret information, and the encryption unit, when authentication is successful, encrypts the content key using the shared session key (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 24, a content storage unit operable to store therein a content key and an encrypted content encrypted using the content key; an encryption unit operable to encrypt the content key using a key generated based on the common secret information, to generate an encrypted content key; and a writing unit operable to write the encrypted content and the encrypted content key to a portable recordable medium (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 25, the received registration request includes an identifier identifying the member device, and the encryption unit encrypts the content key using a key generated based on the common secret information and the identifier, to generate the encrypted content key (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 26, the encryption unit encrypts the content key using a key generated based on the common secret information and an identifier unique to the portable recordable medium (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 27, a holding unit operable to hold, in correspondence with identifiers that each identify a different group, (i) common secret information unique to the group and (ii) a maximum number of member devices registerable in the group, wherein the received registration request includes one of the identifiers, the judging unit, on receipt by the reception unit of the registration request, judges whether the number of member devices registered in a group identified by the identifier is less than a

maximum number corresponding to the identifier, and when judged in the affirmative, registers the member device in the group and selects common secret information corresponding to the identifier, and the communication unit outputs the selected common secret information to the member device (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

With respect to claim 34, a determining unit operable, after the outputting of the common secret information, to determine a member device registered in the group to be another group management device; and a dividing unit operable to divide member devices registered in the group into member devices to be registered in a group managed by the group management device and member devices to be registered in another group managed by the other group management device, and the communication unit outputs, after the dividing by the dividing unit, a different piece of common secret information to the member devices to be registered in the group managed by the group management device (see Yevgeny page 5 lines 11-16, page 7 line 25 – page 8 line 2, page 10 lines 11-16, page 19 line 23 – page 20 line 24).

Claims 3, 30-33, and 69 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huang et al: "Group leader election under-state routing" in view of Yang Y R et al: "Reliable Group Rekeying: A Performance Analysis". With respect to claim 69, Huang teaches a group management device that manages a group , comprising: a reception unit operable to receive, from a member device, a request for registration in the group; a judging unit operable, (i) upon receiving the request, if the

member device is authenticated as being a legitimate device, to judge whether a registered number of member devices is less than a maximum number of member devices registerable in the group, a communication unit operable, when judged in the affirmative, to output to the member device, the common secret information (see Huang chapter 2.2). Huang does not teach (ii) when judged in the affirmative, to issue valid period information showing a valid period of use of common secret information unique to the group for the member device, and to increase the registered number, and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends; and to output to the member device, the valid period information. Yang teaches (ii) when judged in the affirmative, to issue valid period information showing a valid period (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. rekey interval T (is the amount of time the key is valid)) of use of common secret information unique to the group for the member device (see chapter 4 tradeoffs of bandwidth overhead and rekey interval i.e. key and chapter 4.3 System constraints and algorithm), and to increase the registered number (see chapter 2.4 Batch rekeying algorithms i.e. Strategy 1), and (iii) to monitor an elapse of the valid period and reduce the registered number when the valid period ends (see chapter 4 tradeoffs of bandwidth overhead and rekey interval and chapter 4.3 System constraints and algorithm); and to output to the member device, the valid period information (see chapter 1 introduction i.e. the group key is controlled by a group management system, which sends the group key to authorized new users and chapter 4.3 System constraints and algorithm). It would have been obvious at the time the invention was made to a person having ordinary skill in the

art to which said subject matter pertains to have the rekey interval as a system design parameter that a group key management system can use to control bandwidth overhead (see chapter 4.3 System constraints and algorithm). Therefore one would have been motivated to have the common secret have a valid period.

With respect to claim 3, upon receiving the request, if the member device is authenticated as being the legitimate device, the judging unit judge whether the registered number of member devices is less than a maximum number of member devices registerable in the group, and when the judged in the affirmative, the judging unit registers the member device (see Huang chapter 2.2).

With respect to claim 30, when the group management device is determined to be a new group management device for managing a new group formed by combining groups managed by a plurality of group management devices, the communication unit outputs to member devices registered in the groups, new common secret information unique to the new group, and when one of the other group management devices is determined to be the new group management device, the group management device further comprises: a receiving unit operable to receive the new common secret information from the other group management device; and a holding unit operable to hold the received new common secret information (see Huang chapter 2.2).

With respect to claim 31, the communication unit determines in conjunction with the other group management devices, one of the group management devices to be the new group management device (see Huang chapter 2.2).

With respect to claim 32, the holding unit stores therein a priority level of the group management device, and the communication unit determines, out of the stored priority level and priority levels of the other group management devices, the group management device having the highest priority level to be the new group management device (see Huang chapter 2.2).

With respect to claim 33, each member device registered in the groups managed by the group management device and the other group management devices has a priority level, and when the group management device is determined to be the new group management device, the reception unit acquires the priority levels of the member devices, the group management device further comprises a selecting unit operable to select, in order from highest to lowest of the acquired priority levels, member devices for registration in the new group, the selected number of member devices being less than or equal to a maximum number of member devices registerable in the new group, and the communication unit outputs the new common secret information to the selected member devices (see Huang chapter 2.2).

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Devin Almeida whose telephone number is 571-270-1018. The examiner can normally be reached on Monday-Thursday from 7:30 A.M. to 5:00 P.M. The examiner can also be reached on alternate Fridays from 7:30 A.M. to 4:00 P.M.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron, can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DA

Devin Almeida
Patent Examiner
5/8/07

GILBERTO BARRON JR
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100